



Programa lectivo

Charlas de ciberseguridad y privacidad digital

Sesiones prácticas para entender riesgos digitales reales, proteger información sensible y adoptar hábitos de seguridad aplicables desde el primer día.

PROPUESTA

Formación clara, útil y accionable

Diseñada para empresas, asociaciones, centros educativos, equipos profesionales y personas que necesitan criterio práctico ante amenazas cotidianas.

1 Formato

Charla divulgativa, taller práctico o formación a medida según el público y el objetivo.

2 Enfoque

Lenguaje comprensible, ejemplos reales y una lista final de acciones prioritarias.

3 Dirigido a

Equipos no técnicos, profesionales expuestos y grupos que gestionan información sensible.



Xabier Durruti

Ciberseguridad · OSINT · Peritaje informático · Privacidad digital

www.xabierdurruti.eus

OBJETIVO

Qué busca la sesión

Concienciar y mostrar medidas de protección frente a amenazas y ataques informáticos que afectan tanto al trabajo como al uso personal de dispositivos.

Descripción

El contenido está pensado para que las personas asistentes entiendan riesgos reales, reconozcan señales de alerta y sepan aplicar buenas prácticas de protección sin depender de conocimientos técnicos avanzados.

Al finalizar

- Identificar correos, enlaces y comportamientos sospechosos.
- Mejorar la seguridad de cuentas, dispositivos y redes.
- Entender el valor de metadatos, cifrado y copias.

Formatos recomendados

A

Charla divulgativa

60-90 minutos para una visión clara de riesgos, errores comunes y hábitos seguros.

B

Taller práctico

2-3 horas con revisión guiada de cuentas, metadatos, dispositivos, copias y exposición pública.

C

A medida

Contenido ajustado al perfil del equipo, sector, exposición pública y necesidades concretas.

Metodología de trabajo

1

Contexto

Perfil del grupo, nivel técnico, riesgos reales y objetivo de la sesión.

2

Aplicación

Ejemplos claros, casos habituales y recomendaciones aplicables desde el primer día.

3

Cierre

Lista de prioridades: qué revisar, qué cambiar y qué dejar documentado.

TEMARIO

Contenidos principales

El programa se organiza por bloques para que la sesión sea fácil de seguir y cada tema tenga una aplicación práctica.

Amenazas y atacantes

- Hackers y tipos de ciberdelincuentes.
- Malware y principales familias de malware.
- Ciberataques en tiempo real, Oday y evasión avanzada.

Ingeniería social

- Ataques basados en contacto humano.
- Ataques basados en informática y telefonía móvil.
- Señales de manipulación, urgencia y suplantación.

Correo, enlaces y navegación

- Diferenciar y analizar una dirección de correo electrónico.
- Analizar posibles correos maliciosos.
- Verificar enlaces y comprobar autenticidad.
- Navegación segura: VPN y redes Wi-Fi.

Dispositivos e información

- Importancia de cifrar pendrives, discos duros y teléfonos móviles.
- Copias, recuperación y respuesta inicial ante incidentes.
- Separación de usos personales y profesionales.

Privacidad y exposición digital

- Google My Activity y actividad asociada a cuentas.
- Metadatos en documentos, imágenes y archivos compartidos.
- Huella pública, perfiles y publicación responsable.

Idea central

Menos miedo y más criterio: reconocer riesgos, decidir mejor y proteger información sensible con hábitos sostenibles.

XABIER DURRUTI

Perfil profesional

Formación y experiencia orientadas a privacidad digital, ciberinteligencia, OSINT, análisis forense y protección de información.

Formación, certificaciones y colaboración

- Play It Safe: Manage Security Risks (Google).
- Foundations of Cybersecurity (Google).
- Connect and Protect: Networks and Network Security (Google).
- HUMINT (LISA Institute - Seguridad, Inteligencia, Ciberseguridad y Geopolítica).
- Advanced Cybersecurity Program (Stanford University).
- Experto universitario en peritaje e informática forense (Universidad UNIR).
- Técnico especialista en ciberinteligencia (Hack by Security).
- Socio y colaborador de Proton (Suiza).
- 2017-2018: Comisión para la Promoción del Euskera en el Medio Digital del Consejo Asesor del Euskera (Gobierno Vasco).

Material necesario

- Proyector con salida HDMI.
- Conexión de red eléctrica para ordenador.
- Ordenador portátil o CPU con HDMI, teclado y ratón para demostraciones.
- Cada asistente puede traer un dispositivo para comprobaciones o ejemplos.

Inversión**200 €**

Información y disponibilidad

www.xabierdurruti.eus